



COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

July 27, 2006

To: Mayor Michael D. Antonovich
Supervisor Zev Yaroslavsky, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Yvonne B. Burke
Supervisor Don Knabe

From: Jon W. Fullinwider
Chief Information Officer

Subject: **UPDATE ON COMPUTER SECURITY INCIDENTS AT COMMUNITY DEVELOPMENT COMMISSION (CDC) AND DEPARTMENT OF COMMUNITY AND SENIOR SERVICES (DCSS)**

On July 21, 2006, I reported to your Board that an Internet-based attack had occurred on a CDC computer system that resulted in the potential exposure of approximately 4800 Housing Management Division tenants' personal information to unknown persons or organizations. CDC retained the services of a forensic expert to determine, more specifically, what data was accessed and what vulnerabilities existed that allowed the unauthorized access to occur. The investigation is still in process; however, preliminary results indicate that the perpetrators were unable to access any specific data records. While log records show that the server was accessed, they also indicate that there were numerous failed attempts to access data records in the system. Pending the results of the investigation, CDC has identified the necessary steps and actions to notify the housing tenants; however, they will not take any action to begin notification until they receive the final results of the investigation which is anticipated within the next two (2) days.

On the weekend of July 22-23, the Burbank and Glendale offices of the Department of Community and Senior Services (DCSS) were burglarized along with other tenants in the building. Eleven (11) DCSS laptop computers were stolen. The laptop computers contained sensitive information regarding Adult Protective Services constituents. This data was used by DCSS social workers in their interactions with clients. Each laptop contained a varying number of records depending on the social worker's caseload. Current estimates are that the eleven (11) laptops contained approximately 216 client records containing confidential/sensitive data.

DCSS filed a police report, notified the Auditor-Controller County Investigations Office, County Counsel and the CIO. Staff began preparing for client notification by identifying the client records involved. On July 26, the Burbank Police Department received a call

from the Riverside Police Department who notified them that they had recovered two of the laptops during a routine traffic stop. While the two (2) laptops will be returned, DCSS will still begin formal notification to all 216 clients, since unauthorized data access on the two laptops recovered cannot be ruled out.

My office in conjunction with department security officers is developing processes and supporting policies that can be employed within the County to mitigate future occurrences of these types of events. Three policies are being finalized for your Board's approval that includes:

- Protection of Information on Portable Computing Devices
- Security Incident Reporting
- Employee Security Awareness

Each of these policies is required to improve the protection of County sensitive information. The policy for information on portable computing devices will require that encryption be implemented on all County-owned portable computing devices regardless of the data that it may contain. We have also commissioned a County technical team to complete requirements for a County encryption standard and have developed an RFP to secure the required software. It is our plan to have the policies reviewed by Department Heads, approved by the Audit Committee, and before your Board for approval by the end of August 2006. During the ensuing timeframe, we will have issued the RFP and selected a vendor to provide a standardized solution for encrypting data on all County laptops. Departments will then be notified that they will need to acquire the encryption software and install it on all laptop computers. Those departments/individuals using PDA's (i.e., Blackberry's, Trio's, etc.) that contain sensitive/confidential data must acquire encryption software to ensure data is secured/protected in the event the device is lost or stolen.

My office will continue to provide status information on the investigation, remediation and notification process as actions are taken and we have a better understanding of the two events in question. Additionally, we have made it our top priority to complete the policies, gain your Board's approval and implement the encryption software on all portable/laptop computers.

JWF:AB:ygd

c: David E. Janssen, CAO
Cynthia Banks, Director, DCSS
Raymond G. Fortner, Jr., County Counsel
Sachi A. Hamai, Executive Officer, Board of Supervisors
Carlos Jackson, Executive Director, CDC
Dave Lambertson, Director, ISD
J. Tyler McCauley, Auditor-Controller